REMARKS/ARGUMENTS

Applicant thanks the Examiner for considering the reference that was filed without an additional IDS.

1.) Claim Amendments

The Applicant has amended claims 1 and 31. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-23, and 31 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 112

Claims 1-22 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant respectfully traverses.

The preamble previously recited "A method...at a gateway node forming a gateway between the two environments, the method comprising". The Applicant has again amended claim 1 to even more clearly recite that the method is performed at the gateway node.

3.) Claim Rejections – 35 U.S.C. § 102(a)

Claims 1-4, 6-16, 19-20, 22, 23, and 31 are rejected under 35 U.S.C. 102(a) as being anticipated by Host Identity Protocol: Achieving IPv4 - Ipv6 handovers without tunneling" by Wall et al. (hereinafter Wall). Applicant respectfully disagrees.

The Examiner's attention is directed to the fact that Wall does not disclose at least "storing the identifier at the gateway node", as recited in independent claims 1, 23, and 31. The Examiner cites Figure 2 of Wall as teaching this element.

Figure 2 of Wall discloses a four way handshake.

"The negotiating parties are named as the Initiator starting the connection and the Responder. The Initiator begins the negotiation by sending an I1 packet,

basically containing the HITs of the nodes participating in the negotiation. The destination HIT may also be zeroed, if the Responder's HIT is not known by the Initiator.

When the Responder gets the I1 packet, it sends back an R1 packet that contains a puzzle to be solved by the Initiator. The protocol is designed so that the initiator must do most of the calculation during the puzzle solving. This gives some protection against DoS attacks. The R1 initiates also the Diffie-Hellman procedure, containing the public key of the Responder together with the Diffie-Hellman parameters.

Once received the R1 packet, the Initiator solves the puzzle and sends the response cookie in an I2 packet together with an IPsec SPI value and its encrypted public key to the Responder. The Responder verifies that the puzzle has been solved, authenticates the Initiator and creates the IPsec ESP SAs. The final R2 message contains the SPI value of the Responder." (Wall, page 3, col. 2, ¶ 2-4)

A close reading of the Wall reference with respect to Figure 2 does not provide a teaching, disclosure, or suggestion of "storing the identifier at the gateway node". Figure 2 only discloses an I1 packet that is sent from an Initiator to a Responder.

The Examiner has read the host identity tag (HIT) of Wall on the identifier of Applicant's claims. However, Wall teaches that "[t]he HITs, which the applications use, must be mapped to the corresponding IP addresses **before** any packets leave the host. (See Wall, II. Host Identity Protocol, B. A New Layer) As such, it can also be argued that Wall also fails to teach "associating an identifier with the first host at the gateway node", as recited by Applicant's independent claims since Wall teaches that its HIT is mapped to the corresponding IP address before it leaves the host. As such, Wall fails to teach what is recited by independent claims 1, 23, and 31.

Therefore, claims 1, 23, and 31 are patentable over the cited art of record. Claims 2-4, 6-16, 19, 20, and 22 are patentable at least by virtue of depending from their respective base claim.

4.) Claim Rejections – 35 U.S.C. § 103 (a)

A. Claim 5

Claim 5 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Wall in view of USP Application Publication 2004/0091117 to Narayanan (hereinafter Narayanan).

Narayanan discloses managing and distributing keys between routers using protocol exchange messages between routers as key distribution vehicles. According to one embodiment of the invention, a router of an autonomous system uses its private key to send cryptographic information associated with another router to a peer router as part of its protocol exchange messages. The peer router is able to extract the cryptographic information and store it in a look-up table. Such protocol exchange messages may occur as part of an Interior Gateway Protocol or an Exterior Gateway Protocol. According to another embodiment of the invention, a chain authentication system is created as boundary routers of autonomous systems having a trust relationship share cryptographic information for other autonomous systems as part of protocol exchange messages for the exterior gateway protocol. (Narayanan, Abstract)

The Examiner concedes that Wall fails to teach that one host is not a HIP enable host. (See Office Action dated 10/22/2008; page 11) In order to cure the Examiner's perceived deficiencies, Narayanan is cited.

As stated above in Section 6.), Wall fails to disclose "storing the identifier at the gateway node" and "associating an identifier with the first host at the gateway node". Narayanan does not cure these deficiencies. As such, claim 5 is patentable over the combination of Wall and Narayanan.

B. Claims 17, 18, and 21

Claims 17, 18, and 21

Claims 17, 18, and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wall in view of USP Application Publication 2002/0057662 to Lim.

Lim discloses multicasting/broadcasting IP data in a mobile communication system, includes the steps of a packet data serving node (PDSN) receiving multicast packet data, transforming the multicast packet data to a PPP frame format having an identification header, transmitting multicast message to base station controller/packet control function (BSC/PCF), the BSC/PCF transmitting multicasting/broadcasting message to all or some of base stations under control of the BSC/PCF according to header information of the multicast message, and transmitting the multicasting/broadcasting message to mobile station through broadcasting channel. (Lim, Abstract)

The Examiner concedes that Wall fails to disclose a 3G mobile environment, a UMTS mobile environment, and a GGSN. In order to cure the Examiner's perceived deficiencies, Lim is cited.

As stated above in Section 6.), Wall fails to disclose "storing the identifier at the gateway node" and "associating an identifier with the first host at the gateway node". Lim does not cure these deficiencies. As such, claim 5 is patentable over the combination of Wall and Lim.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

Date: September 2, 2009

Thomas Bethea, Jr.
Reg. No. 53,987

Ericsson Inc.
6300 Legacy Drive
M/S EVR 1-C-11
Plano, TX 75024
972-583-4859
thomas.bethea.jr@ericsson.com